Plan Overview

A Data Management Plan created using dmptool

Creator: Carrie Seigler

Affiliation: Princeton University

Funder: National Science Foundation (NSF)

Template: NSF-SBE: Social, Behavioral, Economic Sciences

Project abstract:

The purpose of this research is to understand the experiences of survivors of sexual violence. Long-term sequelae and reactions to sexual abuse can vary greatly; much of this variance has been attributed to environmental factors such as family structure and socioeconomic status as well as individual factors such as "grit" or "resilience" (Ewing 1998). However, little has been done to study the ways in which religious identities might influence different coping strategies and subsequent life trajectories after abuse. Most research examining the intersection of religion and trauma has been generated by scholars in the applied fields of psychology, psychiatry, and social work. The extant studies examining the direct link between trauma and religious beliefs number a scant eleven in total, often involve only one informant, and collectively present mixed findings on the matter (Chen and Koenig, 2006). While previous studies suggest that traumatic events might subsequently impact survivors' religious beliefs, this nascent line of inquiry has yet to be taken up in earnest by sociologists. The proposed study seeks to fill the void in the research by examining the interaction between sexual abuse, the construction of religious identities, and processes of meaning-making on a broader social scale. (For a thorough review of the literature on sexual trauma as it relates to religious beliefs see Leo, Darius, Zahra Izadikhah, Erich C. Fein, and Sayedhabibollah Ahmadi Forooshani. 2019. "The Effect of Trauma on Religious Beliefs: A Structured Literature Review and Meta-Analysis." Trauma, Violence, & Abuse. doi: 1524838019834076.)

Last modified: 03-16-2021

Religion and Sexual Violence

Roles and responsibilities

The DMP should outline the rights and obligations of all parties as to their roles and responsibilities in the management and retention of research data. It should also consider changes to roles and responsibilities that will occur should a principal investigator or co-PI leave the institution or project. Any costs should be explained in the Budget Justification pages.

Carolina Seigler will be the primary researcher tasked with collecting, reviewing, analyzing, managing, and retaining the data as well as the metadata for this project. The research protocol also allows Timothy Nelson (PI), Kathryn Edin (research personnel), and Matthew Desmond (research personnel) to access and review the data after it has been sufficiently anonymized. All personnel have past research experience with collecting and managing sensitive data, specifically data from in-depth interviews with vulnerable persons. The graduate student researcher also has had experience protecting sensitive qualitative data (narrative accounts of sexual assault) and managing these data across national borders (USA – Botswana). Researchers will ensure that all research personnel have thoroughly read and understand the study protocol. All researchers have received ethics training and certification per University guidelines.

Expected data

The DMP should describe the types of data, samples, physical collections, software, curriculum materials, and other materials to be produced in the course of the project. It should then describe the expected types of data to be retained.

This study will generate data primarily through (1) participant observations of support groups for those abused by clergy and (2) in-depth, semi-structured interviews with these individuals. Until in-person research may safely resume, data will be collected via phone calls and video calls hosted on encrypted and passcode-protected conferencing platforms.

Data will be collected in the form of audio recordings (collected on an external recording device free of any network connections), transcriptions of these recordings, physical notes taken during participant observation sessions, and any documents (e.g., email correspondences, scanned copies of letters or photographs) that respondents voluntarily choose to share with the researchers. All data in this study will be de-identified and associated with an anonymizing alpha-numeric code. See “Data Format and Dissemination” for information on privacy and security.

Data will be imported into a qualitative or mixed-methods analysis software. When using this software to access and analyze data, researchers will use a password protected device that they will either (1) connect to the Princeton University VPN via two-factor authentication or (2) disconnect from all networks while in use. Researchers will also produce metadata describing all collected materials as well as the alpha-numeric schema researchers will use to systematically pseudonymize any personally identifiable information (PII). It is anticipated that the data, metadata, and analysis files will together demand about 100 GB of storage.

Period of data retention

SBE is committed to timely and rapid data distribution. However, it recognizes that types of data can vary widely and that acceptable norms also vary by scientific discipline. It is strongly committed, however, to the underlying principle of timely access, and applicants should address how this will be met in their DMP statement.

Data will be maintained on an external hard drive (password protected, free from all network connections, and kept in a locked drawer of a researcher’s locked office) for a minimum of three

years after the conclusion of the award. However, given the sensitivity of these data, the research team anticipates the period of protection and retention to extend well past this minimum.

Data format and dissemination

The DMP should describe data formats, media, and dissemination approaches that will be used to make data and metadata available to others. Policies for public access and sharing should be described, including provisions for appropriate protection of privacy, confidentiality, security, intellectual property, or other rights or requirements. Research centers and major partnerships with industry or other user communities must also address how data are to be shared and managed with partners, center members, and other major stakeholders.

Digital audio files will be processed in MP3 format and saved as password protected files using the naming convention year, month, day, alpha-numeric pseudonym code, and approximate time of original recording. Interview transcripts will be saved as password protected DOCX files using the same naming convention. Once imported into the data analysis software they will be saved as password protected files in that software's unique format. Metadata and anonymization keys will be saved as password protected XLSX files.

Physical documents received from participants via mail will be scanned and retained as password protected items before being stored in a locked cabinet of a researcher's locked office. Digital data received from participants via email will be saved as passcode protected items matching the format of the file received. The research team anticipates that most of these data will be preserved in DOCX, JPG, MP3, PDF, PNG, TXT, or XLSX format.

The researchers and institutional review board have determined that this study presents the highest level of risk to research participants. At this time, the researchers do not anticipate sharing interview transcripts, records, and notes with the study participants, nor do they plan to make these data available to the wider scientific community. While this study is supported by NSF funding, meaning that the NSF's public access policy does apply here, legal and ethical restrictions impinge upon the researchers' ability to freely share these data with others.

At the May 2016 workshop "Public Access to NSF-Funded Research Data for the Social, Behavioral, and Economic Sciences," several experts remarked that some data – particularly certain qualitative data – may be "so sensitive that data sharing is ill-advised." Sensitivity factors present in this research indeed limit the ability to publicly share the data collected. This study collects sensitive PII pertaining to incidents of sexual trauma. Even with rigorous deidentification procedures in place, the risk of deductive disclosure is still great if these qualitative data were to be made publicly available. Additionally, it is anticipated that at the time of data collection several respondents will be involved in active legal disputes concerning these incidents. The research team has acquired a Certificate of Confidentiality through the NIH (2020 August). However, this certificate primarily protects the *researchers* from having to disclose names or identifying characteristics of research subjects in response to legal demands. Even with this certificate, the research subjects *themselves* remain at risk as long as sensitive data on their personal experiences with sexual trauma are available and possibly attainable by parties seeking to interfere with their legal proceedings.

The researchers are confident that they have put in place provisions for appropriate protection of the research subjects' privacy and confidentiality. However, given the highly sensitive nature of this study as well as the enduring ethical debates surrounding access to sensitive qualitative data, the researchers do not plan to disseminate these data for public use. A breach of confidentiality could potentially cause great psychological, emotional, or personal harm if otherwise private accounts of sexual violence were to be connected to their identity. To respect the participants' rights to be free from unreasonable intrusion, including control over the extent, timing, and circumstances of obtaining personal information about them, only the research personnel associated with this project will be granted access to these data.

Data storage and preservation of access

The DMP should describe physical and cyber resources and facilities that will be used for the effective preservation and storage of research data. These can include third party facilities and repositories.

Given the sensitive nature of these data, it is not anticipated that researchers will utilize cloud services in this study, nor that data will be transferred during this study.

All data and metadata developed during this study will be stored on password protected and encrypted research spaces. Digital data will be accessible only through servers requiring multifactor authentication utilizing a mechanism approved by Princeton's sociology department and Office of Information Technology. A backup of these data will be stored on an external hard drive that is password protected, free from all network connections, and kept in a locked drawer in a researcher's locked office. Physical documents acquired throughout the data collection period will be kept in a location separate from other research data in a different locked container in a researcher's locked office.

Additional possible data management requirements

More stringent data management requirements may be specified in particular NSF solicitations or result from local policies and best practices at the PI's home institution. Additional requirements will be specified in the program solicitation and award conditions. Principal Investigators to be supported by such programs must discuss how they will meet these additional requirements in their Data Management Plans.

Additional data protection measures: It would be imprudent to conduct this research as it has been defined by its specific aims and objectives if the researchers required written consent from participants. To further protect the privacy of research subjects, researchers will not collect written documentation of consent. The IRB has approved this waiver as the only record linking the subject and the research would be the informed consent form and the principal risk would be potential harm resulting from a breach of confidentiality.

To protect against unauthorized access during the virtual data collection period (including but not limited to online threats, unwelcomed messages or images, harassment, or attempts to "Zoom bomb" conference calls), researchers will follow Princeton University's guidelines to proactively ensure the security of online interview sessions. Additionally, the study's recruitment and information website will feature a high security clearance with Secure Sockets Layer (SSL), redirect to Hypertext Transfer Protocol Secure (HTTPS) after the certificate is issued even if respondents enter through a less secure HTTP address, include HTTPS links for all sitemaps, appear only under the HTTPS version in search engine indices, and remain inaccessible in browsers that do not support SSL. Any PII submitted through the website's recruitment or interest forms will be delivered to an email address accessible only through two-factor authentication. All emails sent from the researchers will be delivered in confidential mode and automatically destroyed after a certain amount of time.

Additional notes on NSF requirements: While the NSF GRFP itself does not require a separate DMP upon application, this research is supported by NSF funds. This DMP therefore adheres as closely as possible to the NSF's policies for the dissemination and sharing of research results for Social, Behavioral and Economic Sciences. A link to these requirements is found here: https://www.nsf.gov/bfa/dias/policy/dmp.jsp

Any suspected breach of PII that occurs within the context or scope of the researcher's NSF award will be reported to the appropriate offices at both Princeton University and the NSF within seven calendar days of the researcher's knowledge of the incident. Researchers will alert their institution's Director of the Office of Research and Project Administration and Chief Information Security Officer at the Office of Information Technology as well as personnel in the Office of Research Integrity and Assurance. Researchers will begin communications with NSF by reaching out to the Chief Information Officer followed by personnel in the Policy Office.

The researchers will cooperate and freely exchange information with these offices as needed to properly escalate, refer, and respond to a breach. They will together validate the scope and nature of the incident and establish an appropriate response plan.

As per NSF requirements, data management will be monitored through the normal Annual and Final Report process. Annual reports will provide information on the progress of data management and sharing of research products. At the end of this multi-year award (fellowship year 2023), the Final Project Report will discuss execution and any updating of the original DMP. This discussion will describe the data produced during the five-year award, data to be retained after the award ends, and any changes to the data sharing protocol. Data management will also be reported in any subsequent NSF-funded proposals under "Results of prior NSF support."